

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person, by name and address)
THE RESIDENCE LOCATED AT
1170 ESSEX GLENN, MORROW,
OHIO 45152.

Case No. 1:21-mj-159

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

18 U.S.C. §§ 1512(c)(2) (obstruction of Congress); 1519 (obstruction of justice – destruction of evidence); 111 (assaulting a federal agent); 231 (civil disorders); 371 (conspiracy); 372 (conspiracy to impede/assault federal agents); 641 (theft of government property); 930 (possession of firearms and dangerous weapons in federal facilities); 1361 (destruction of government property); 1752(a) (unlawful entry on restricted buildings or grounds); 2101 (interstate travel to participate in riot); 2383 (rebellion or insurrection); and 2384 (seditious conspiracy); and 40 U.S.C. § 5104(e)(2) (violent entry, disorderly conduct, and other offenses on capitol grounds)

The application is based on these facts:

Please See Attached Affidavit

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature


Special Agent T. A. Staderman II, FBI

Printed name and title

Sworn to before me and signed in my presence.
via FaceTime video

Date: 02/17/2021

City and state: Cincinnati, Ohio


Karen L. Litkovitz
United States Magistrate Judge



IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF
THE RESIDENCE LOCATED AT
1170 ESSEX GLENN, MORROW, OHIO
45152.

Case No. 1:21-mj-159

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, **T. A. Staderman II**, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 1170 Essex Glenn, Morrow, Ohio, hereinafter "PREMISES," further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the FBI and have been so employed since 2008. As a Special Agent with the FBI, I am empowered by law to conduct investigations, make arrests, and execute and serve search and arrest warrants for offenses enumerated in Title 21 and Title 18 of the United States Code. As a Special Agent, I have been assigned to investigate various Domestic and International Terrorism matters. Through my training, education and experience, I have become familiar with the manner in which criminal activity is carried out, and the efforts of persons involved in such activity to avoid detection by law enforcement.

3. Unless otherwise stated, the information in this Affidavit is either personally known to me, has been provided to me by other individuals, or is based on a review of various documents, records, and reports. Because this Affidavit is submitted for the limited purpose of establishing

probable cause to support an application for a search warrant, it does not contain every fact known by me or the United States. The dates listed in this Affidavit should be read as “on or about” dates.

4. This investigation concerns alleged violations of 18 U.S.C. §§ 1512(c)(2) (obstruction of Congress); 1519 (obstruction of justice – destruction of evidence); 111 (assaulting a federal agent); 231 (civil disorders); 371 (conspiracy); 372 (conspiracy to impede/assault federal agents); 641 (theft of government property); 930 (possession of firearms and dangerous weapons in federal facilities); 1361 (destruction of government property); 1752(a) (unlawful entry on restricted buildings or grounds); 2101 (interstate travel to participate in riot); 2383 (rebellion or insurrection); and 2384 (seditious conspiracy); and 40 U.S.C. § 5104(e)(2) (violent entry, disorderly conduct, and other offenses on capitol grounds) (the “Subject Offenses”), stemming from the conduct of a certain sub-set of the individuals who stormed the U.S. Capitol on January 6, 2021, as well as those who aided and abetted and conspired with that sub-set of individuals who attacked the U.S. Capitol.

PURPOSE OF AFFIDAVIT

5. I respectfully submit that this Affidavit establishes probable cause to believe that evidence of Sandra Parker’s and Bennie Parker’s involvement in the Subject Offenses is located at the PREMISES.

6. On and about January 6, 2021, Sandra Parker, dressed in a uniform consisting of camouflaged-combat attire, and, operating as a group with several other similarly-attired members of the “Oath Keepers Militia,” breached the U.S. Capitol, directly or indirectly damaged property of the Capitol, and obstructed Congress’s proceedings. Bennie Parker, similarly dressed in a uniform consisting of camouflaged-combat attire, assisted Sandra Parker and other members of

the “Oath Keepers Militia” by attempting to stay in communication with those members who were inside the Capitol.

BACKGROUND

The 2020 United States Presidential Election and the Official Proceeding on January 6, 2021

7. The 2020 United States Presidential Election occurred on November 3, 2020.

8. The United States Electoral College is a group required by the Constitution to form every four years for the sole purpose of electing the president and vice president, with each state appointing its own electors in a number equal to the size of that state’s Congressional delegation.

9. On December 14, 2020, the presidential electors of the U.S. Electoral College met in the state capital of each state and in the District of Columbia and formalized the result of the 2020 U.S. Presidential Election: Joseph R. Biden Jr. and Kamala D. Harris were declared to have won sufficient votes to be elected the next president and vice president of the United States.

10. On January 6, 2021, a Joint Session of the United States House of Representatives and the United States Senate (“the Joint Session”) convened in the United States Capitol building (“the Capitol”) to certify the vote of the Electoral College of the 2020 U.S. Presidential Election (“the Electoral College vote”).

The Attack at the U.S. Capitol on January 6, 2021

11. The Capitol is secured 24 hours a day by United States Capitol Police. The Capitol Police maintain permanent and temporary barriers to restrict access to the Capitol exterior, and only authorized individuals with appropriate identification are allowed inside the Capitol building.

12. On January 6, 2021, at approximately 1:00 p.m., the Joint Session convened in the Capitol building to certify the Electoral College vote. Vice President Michael R. Pence, in his constitutional duty as President of the Senate, presided over the Joint Session.

13. A large crowd began to gather outside the Capitol perimeter as the Joint Session got underway. Crowd members eventually forced their way through, up, and over Capitol Police barricades and advanced to the building's exterior façade. Capitol Police officers attempted to maintain order and stop the crowd from entering the Capitol building, to which the doors and windows were locked or otherwise secured. Nonetheless, shortly after 2:00 p.m., crowd members forced entry into the Capitol building by breaking windows, ramming open doors, and assaulting Capitol Police officers. Other crowd members encouraged and otherwise assisted the forced entry. The crowd was not lawfully authorized to enter or remain inside the Capitol, and no crowd member submitted to security screenings or weapons checks by Capitol Police or other security officials.

14. Shortly thereafter, at approximately 2:20 p.m., members of the House and Senate (including Vice President Pence)—who had withdrawn to separate chambers to resolve an objection—were evacuated from their respective chambers. The Joint Session and the entire official proceeding of the Congress was halted while Capitol Police and other law-enforcement officers worked to restore order and clear the Capitol of the unlawful occupants.

15. Later that night, law enforcement regained control of the Capitol. At approximately 8:00 p.m., the Joint Session reconvened, presided over by Vice President Pence, who had remained hidden within the Capitol building throughout these events.

16. In the course of these events, approximately 81 members of the Capitol Police and 58 members of the Metropolitan Police Department were assaulted. Additionally, many media members were assaulted and had cameras and other news-gathering equipment destroyed, and the Capitol suffered millions of dollars in damage—including broken windows and doors, graffiti, and residue of various pepper sprays, tear gas, and fire extinguishers deployed both by crowd members who stormed the Capitol and by Capitol Police officers trying to restore order.

The Oath Keepers Militia

17. Law enforcement and news-media organizations observed that members of a paramilitary organization known as the Oath Keepers were among the individuals and groups who forcibly entered the U.S. Capitol on January 6, 2021. The Oath Keepers are a large but loosely-organized collection of militia that believe that the federal government has been coopted by a shadowy conspiracy that is trying to strip American citizens of their rights. Though the Oath Keepers will accept anyone as members, what differentiates them from other anti-government groups is their explicit focus on recruiting current and former military, law enforcement, and first-responder personnel. The organization's name alludes to the oath sworn by members of the military and police to defend the Constitution "from all enemies, foreign and domestic." The Oath Keepers are led by Person One.

18. In a widely disseminated video¹ recorded by a photojournalist on January 6, 2021, a "stack" of individuals dressed in matching uniforms consisting of camouflaged-combat attire, to include confirmed Oath Keeper members (further described below), moves up and through a crowd on the east side of the U.S. Capitol. A screenshot of the video is below, with a portion of the "stack" encircled by a red oval:

¹ See <https://apnews.com/article/ex-military-cops-us-capitol-riot-a1cb17201dfddc98291edead5badc257/gallery/0ecd1781c66d437f92c61b3f4848a74e> (at slide 10).



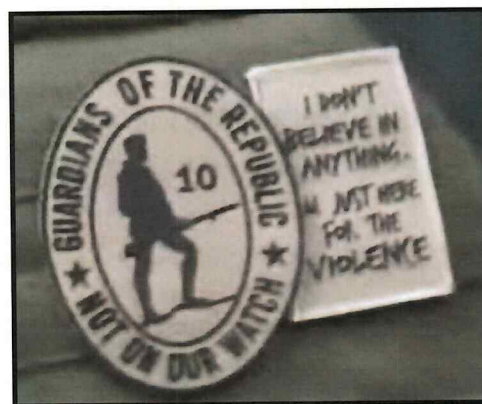
19. Based on my training and experience, a stack or line formation is a tactical formation used by infantryman in the military. One defining feature of this formation is that members keep their hands on the backs or vests of the person in front of them to remain together while entering a room or weaving through a crowd. The purpose of maintaining direct physical contact with one another is to efficiently communicate with one another, especially in crowded or noisy areas.

20. A service called "News2Share" uploaded to YouTube a video of the January 6, 2021, attack at the Capitol. At the approximate 3-minute-and-8-second mark, the video shows eight-to-ten individuals in matching uniforms consisting of camouflaged-combat attire

aggressively approaching an entrance to the Capitol.² These individuals, who are wearing helmets, reinforced vests, and clothing with Oath Keeper logos and insignia, can be seen moving in an organized and practiced fashion and forcing their way to the front of the crowd gathered around a set of doors to the Capitol.



21. A close-up view of the badges on the vest of one of these individuals, seen just under the Oath Keepers emblem on his shirt, displays the Oath Keepers motto, "Not On Our Watch."

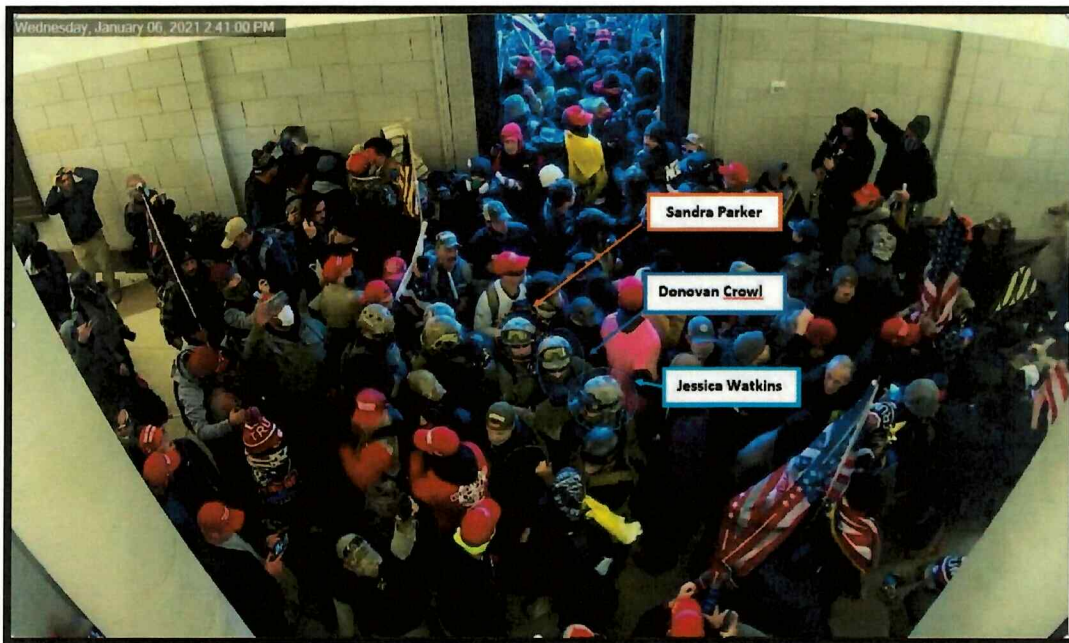


² See <https://www.youtube.com/watch?v=b76KfHB0QO8&feature=youtu.be>.

22. Based on the foregoing observations of the video, and information gained in the course of my investigation, it is reasonable to believe that the organized group of individuals marching to the doors of the Capitol in the video above are members and affiliates of the Oath Keepers.

23. On January 6, 2021, the particular Capitol doors through which this “stack” of Oath Keepers (and other members of the crowd) breached were significantly damaged. Among other damage, multiple panes of glass were smashed, and a door handle was missing or broken off.

24. Surveillance video from inside the Capitol shows this “stack” of Oath Keepers (and other members of the crowd) shortly after they breached and damaged the doors to the Capitol:



25. Members of the “stack” of Oath Keepers that forcibly entered the Capitol then congregated inside the north section of the Rotunda, as seen in surveillance video from inside the Capitol:



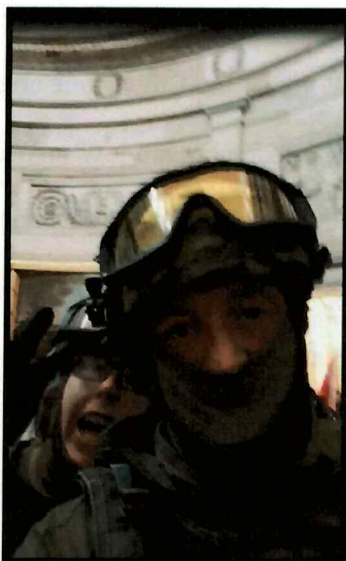
26. Finally, a photojournalist took photos of the members of the “stack” inside the Rotunda as they continued to communicate with one another by keeping their hands on each other’s backs:



The Co-Conspirators

Jessica Watkins & Donovan Crowl

27. Jessica Watkins and Donovan Crowl were among the “stack” members who penetrated the U.S. Capitol Rotunda. In a Parler video compiled by ProPublica,³ Watkins and Crowl are shown together in the Capitol Rotunda. Crowl says, “We took on the Capitol! We overran the Capitol!” Watkins exclaims, “We’re in the fucking Capitol, [unintelligible]!” Watkins and Crowl turn the camera around for a video selfie as they do so:



28. On January 16, 2021, the government obtained a warrant for Watkins’s and Crowl’s arrests from the District Court for the District of Columbia, and a warrant to search Watkins’s home in Woodstock, Ohio, from the District Court for the Southern District of Ohio.

29. On January 17, 2021, FBI agents executed a search warrant of Watkins’s residence. Inside, they located protective equipment and battle gear of the sort worn during the offenses of January 6, 2021 (to include a camouflage hat and jackets; a backpack with medical/PPE supplies;

³ See <https://projects.propublica.org/parler-capitol-videos>.

a black tactical kit with medical supplies, radio, mini drone, and pepper spray; a bag containing a helmet and respirators; and a bag containing a helmet, radio, and belt); cellular telephones; numerous firearms; a paintball gun with rubber-steel balls and a cylinder; pool cues cut down to baton size; zip/cable ties; a recipe for making a destructive device; and other items.

30. That same day, a search of a location where Crowl was said to have occasionally stayed resulted in the recovery of a green reinforced vest. Affixed to the vest was a label with the name “Trapper,” which was a label visible on videos and in photos that captured Crowl during the incursion of the Capitol.

31. Later that day, both Watkins and Crowl were arrested.

32. On January 27, 2021, a federal grand jury in Washington, D.C., indicted Watkins and Crowl, in case number 21-CR-00028, on counts of Conspiracy, in violation of 18 U.S.C. § 371; Obstruction of an Official Proceeding, in violation of 18 U.S.C. § 1512(c)(2); Destruction of Government Property and Aiding and Abetting, in violation of 18 U.S.C. §§ 1361, 2; and Restricted Building or Grounds Access, in violation of 18 U.S.C. §§ 1752(a)(1)-(2).

33. In addition, the FBI has obtained an audio recording of Zello⁴ communications between Watkins and other suspected Oath Keepers during the January 6th attack on the U.S. Capitol. During the recorded transmission—believed to be among Watkins and other Oath Keepers on a Zello channel called “Stop the Steal J6”—Watkins had the following exchanges (among others), which are approximately transcribed:

- a. At the approximate 5-minute mark, the voice believed to be Watkins reports,
“We have a good group. We have about 30-40 of us. We are sticking together

⁴ Zello is a push-to-talk application that operates like a walkie-talkie on a cellular telephone. The Zello application may, depending on a user’s settings, store recordings and other information about the user’s communications on the user’s phone.

and sticking to the plan.” An unknown male responds, “We’ll see you soon, Jess. Airborne.”

- b. At the approximate 7-minute-and-44-second mark, an unknown male states, “You are executing citizen’s arrest. Arrest this assembly, we have probable cause for acts of treason, election fraud.” The voice believed to be Watkins responds, “We are in the mezzanine. We are in the main dome right now. We are rocking it. They are throwing grenades, they are fricking shooting people with paint balls. But we are in here.” An unknown male responds to Watkins, telling her to be safe, and states, “Get it, Jess. Do your fucking thing. This is what we fucking [unintelligible] up for. Everything we fucking trained for.”

Thomas Caldwell

34. Thomas Caldwell conspired with members of the Oath Keepers, including Watkins and Crowl, to go to and storm the U.S. Capitol on January 6, 2021. Notably, Caldwell provided logistical assistance, including finding the hotel in Northern Virginia where several members of the conspiracy stayed from January 5 through 7, 2021. Caldwell further coordinated with a group of co-conspirators who agreed to serve as a “quick reaction force” (“QRF”) to monitor the attack at the Capitol from a distance and be prepared to travel to the Capitol in the event they were called upon, possibly while armed. Caldwell also provided maps informing the QRF team how to most effectively reach the Capitol from their staging area.

35. Caldwell was also present outside of the U.S. Capitol on January 6, 2021. In a YouTube video⁵ recording the events of January 6, 2021, Caldwell is interviewed and, while

⁵ See https://www.youtube.com/watch?v=L5hksM_R59M.

motioning to the Capitol, shouts, “Every single [expletive beeped in original] in there is a traitor. Every single one!”



36. On January 19, 2021, law-enforcement officers searched Caldwell’s home during the execution of a search warrant and recovered a Gadsden “Don’t Tread on Me” flag containing Watkins’s and Crowl’s signatures (among others), a Donald Trump poster with Watkins’s and Crowl’s signatures (among others), and a hand-drawn Oath Keepers insignia above the handwritten words “14 Nov 20 ‘Million MAGA March.’”

37. A federal grand jury in Washington, D.C., indicted Caldwell along with Watkins and Crowl on counts of Conspiracy, Obstruction of an Official Proceeding, Destruction of Government Property, and Entering a Restricted Building or Grounds, in case number 21-CR-00028.

38. The FBI has obtained Facebook records and cellular telephone data that demonstrate how Caldwell, Crowl, Watkins, and others planned and coordinated their efforts to stop, delay, and hinder the certification of the results of the 2020 U.S. Presidential Election:

- a. In the days after the election, Watkins texted with a number of people whom she identified in the contacts list of her phone as a possible “recruit.” Watkins told one of these individuals, “[I]f Biden get the steal, none of us have a chance

in my mind. We already have our neck in the noose. They just haven't kicked the chair yet."

b. Caldwell, Cowl, Watkins, and others attended the "Million MAGA" march, held on November 14, 2021, with the Oath Keepers leader, Person One.

c. After that weekend, Caldwell sent Watkins the following message:

Hi, CAP! Wanted to tell you it was great to have you here in Virginia. Don't know what [Person One] is cooking up but I am hearing rumblings of another Maga March 12 December. I don't know what will happen but like you I am very worried about the future of our country. Once lawyers get involved all of us normal people get screwed. I believe we will have to get violent to stop this, especially the antifa maggots who are sure to come out en masse even if we get the Prez for 4 more years. Stay sharp and we will meet again. You are my kinda person and we may have to fight next time. I have my own gear, I like to be ON TIME and go where the enemy is, especially after dark. Keep the faith! Spy.

d. On December 29, 2020, Watkins texted Cowl to let him know, "We plan on going to DC on the 6th, weather permitting," and when Cowl asked what was happening that day, Watkins responded, "DC. Trump wants all able bodied Patriots to come. I'm sure Tom would love to see us as well. If Trump activates the Insurrection Act, I'd hate to miss it[.]"

e. On December 30, 2020, Watkins and Caldwell exchanged several text messages coordinating their plans and the plans of others for January 6, 2021, including the following message sent by Caldwell to Watkins:

Talked to [Person Three].⁶ At least one full bus 40+ people coming from N.C. Another group (unclear if Mississippi guys) also a bus. Busses have their own lane on the 14th street bridge so they will be able to get in and out. [Person Three] is driving

⁶ This individual is referred to in other filings in this matter as "Person Three," so I am using that nomenclature in this affidavit even though this affidavit does not reference a "Person Two."

plus 1 and arriving nite before. As we speak he is trying to book a room at Comfort Inn Ballston/Arlington⁷ because of its close-in location and easy access to downtown because he feels 1) he's too broken down to be on the ground all day and 2) he is committed to being the quick reaction force and bringing the tools if something goes to hell. That way the boys don't have to try to schlep weps on the bus. He'll bring them in his truck day before. Just got a text from him he WAS able to book a room in that hotel I recommended which is on Glebe Road in Arlington. However it goes it will be great to see you again! I sure hope your arm is getting better!

- f. On December 31, 2020, Caldwell replied to a Facebook comment, writing, "It begins for real Jan 5 and 6 on Washington D.C. when we mobilize in the streets. Let them try to certify some crud on capitol hill with a million or more patriots in the streets. This kettle is set to boil..."
- g. On January 6, 2021, while at the Capitol, Caldwell received the following Facebook message: "All members are in the tunnels under capital seal them in. Turn on gas." When Caldwell posted a Facebook message that read, "Inside," he received the following messages, among others: "Tom take that bitch over"; "Tom all legislators are down in the Tunnels 3floors down"; "Do like we had to do when I was in the core start tearing oit florris go from top to bottom"; and "Go through back house chamber doors facing N left down hallway down steps."
- h. On January 7, 2021, the day after the attack, Caldwell wrote to Crowl, "Did you like the pictures of us storming the castle? I tried calling Cap a lot but it was probably hard for het to hear the phone ring." Crowl responded, "Loved it."

⁷ This is the same hotel at which Caldwell, Watkins, and Crowl stayed, at Caldwell's suggestion.

- i. On January 8, 2021, Crowl sent Caldwell a message asking for a video. Caldwell sent it, and Crowl wrote, “Thank you Sir. Love the hell outta you Tom.” Caldwell responded, “You too, my dear friend! We stormed the gates of corruption together (although on opposite sides of the building) so between that and our first meeting and getting to know you since I can say we will always be brothers!”

Sandra Parker and Bennie Parker

39. Sandra Parker is a 62-year-old resident of Warren County, Ohio. As described more fully herein, Sandra Parker planned with her husband, Bennie Parker, and others known and unknown, to forcibly enter the Capitol on January 6, 2021, and to obstruct the Congressional proceeding occurring that day.

40. Bennie Parker is a 70-year-old resident of Warren County, Ohio. As described more fully herein, Bennie Parker planned with his wife, Sandra Parker, and others known and unknown, to forcibly enter the Capitol on January 6, 2021, and to obstruct the Congressional proceeding occurring that day.

41. As described below, evidence uncovered in the course of the investigation demonstrates that not only did Sandra Parker and Bennie Parker and others conspire to forcibly storm the U.S. Capitol on January 6, 2021—they planned their attack in advance and communicated with one another before, during, and after their attack on the Capitol.

Identification of Sandra Parker and Bennie Parker

42. A search of Watkins’s cellular telephone revealed a contact, “Recruit Ben - OSRM,”⁸ with a telephone number of XXX-XXX-5576 (redacted) that, after an open-source

⁸ On information and belief, OSRM stands for Ohio State Regular Militia.

search, was determined to match the telephone number of Bennie Parker, age 70, with an address located in Morrow, Ohio. A female, Sandra Parker, age 62, was associated with the same address.

43. A query of the Ohio Law Enforcement Gateway confirmed Sandra Parker and Bennie Parker were associated with the same address located in Morrow, Ohio.

Sandra Parker and Bennie Parker Planning For January 6

44. A search of Watkins's cellular phone revealed several text messages between Watkins and "Recruit Ben – OSRM" (believed to be Bennie Parker, as described below).

45. On November 11, 2020, when discussing the Million MAGA March on November 14, 2020, Bennie Parker texted Watkins, "Unfortunately we cant take weapons." Watkins responded approximately one-minute later, "Not into the city, no. Just mace, tasers and nightsticks."

46. On December 27, 2020, Bennie Parker texted Watkins, "I may have to see what it takes to join your militia, our is about gone." Also on December 27, 2020, Bennie Parker texted Watkins, "Yes and you and Sandi and I are like minded you guy aren't that far away"

47. Numerous text messages exchanged between Watkins and Bennie Parker appear to relate to preparations for the trip to Washington D.C. on January 6, 2021, including travel arrangements discussed on December 26 and 27, 2020:

Bennie Parker to Watkins: Is any of your members going to Washington on January 6?

Watkins to Bennie Parker: We are trying to, weather dependant. West Virginia/Maryland mountains are treacherous to drive

Bennie Parker to Watkins: Sandi and I want to go but would like to possibly meet with you and go with you guys. Safety and parking issues to name a few.

Bennie Parker to Watkins: I am seeing now that if you can't make it to

Washington then we should go to our state capital.

Watkins to Bennie Parker: Roger that. Parking is no issue, if you roll with the militia we have a guarded Rally Point

Bennie Parker to Watkins: I'll let Sandi know depends on the weather. Ive herd talk about Columbus if we can't make Washington.

Bennie Parker to Watkins: I'll let you know. Keep me posted on what you all do if you don't mind. Thanks for getting back to me.

48. In further text message communications between Watkins and Bennie Parker on December 29 and 30, 2020, they discussed Oath Keeper membership and meeting in advance to prepare for the January 6, 2021, trip to Washington, D.C.:

Bennie Parker to Watkins: 1/2 Great we need to get together and find out what we need to do to become member, we are retired so we can meet anytime. Also let me know what you all are


Bennie Parker to Watkins: 2/2 doing on the 6th.

Watkins to Bennie Parker: Will do. Right now, considering DC still.

Watkins to Bennie Parker: When would you like to meet up before we go to DC? We work 6 days a week (we own a bar). You could come to our place, or meet up somewhere.

Bennie Parker to Watkins: Yes before would be great and we can come to your place. Let me know when and where.

Watkins to Bennie Parker: When - anytime after 3pm. Where - 102 N. Main St, Woodstock, OH, 43084

Watkins to Bennie Parker: Any day but Sunday is good 

Bennie Parker to Watkins: How about this Saturday?

Watkins to Bennie Parker: Sounds good sir. We convoy out to the Rally Point in Virginia on Tuesday

Bennie Parker to Watkins: Sounds good we will see you Saturday afternoon.

Watkins to Bennie Parker: See you then!

49. On January 3, 2021, Bennie Parker and Watkins discussed the uniforms, gear, and weapons they would wear and bring on January 6, 2021:

Watkins to Bennie Parker: We are not bringing firearms. QRF⁹ will be our Law Enforcement members of Oathkeepers.

Bennie Parker to Watkins: Good to know.

Watkins to Bennie Parker: Pack Khaki/Tan pants. Weapons are ok now as well. Sorry for the confusion. We are packing the car and heading your way shortly

Bennie Parker to Watkins: We don't have any khakis We have jeans and our b d u's¹⁰ So I can bring my gun?

Sandra Parker and Bennie Parker's Participation in the Conspiracy

50. Records obtained from the Comfort Inn Ballston in Arlington, Virginia, confirm that a room was rented for two adults from January 5-7, 2021, by Sandra Parker listing a home address in Morrow, Ohio. Comfort Inn records also establish that individuals named "Thomas Caldwell" and "Jessica Wagkins" each rented a room for two adults at the Comfort Inn Ballston during those same dates.

51. The FBI obtained surveillance video from the Comfort Inn Ballston during the January 5-7, 2021, timeframe. As reflected in the below still frame, this footage shows that on January 5, 2021, Sandra Parker and Bennie Parker (yellow circles) were at the hotel interacting with individuals believed to be Watkins and Crowl (red circles). Sandra Parker is observed

⁹ Based on the investigation, "QRF" appears to be a reference to the "quick reaction force" referenced above.

¹⁰ "B.D.U." is an apparent reference to the military's Battle Dress Uniform, which is a camouflaged combat uniform.

wearing tan pants, a black top, and a tan baseball hat. Bennie Parker is observed wearing tan pants, a burgundy shirt, and a dark baseball hat.



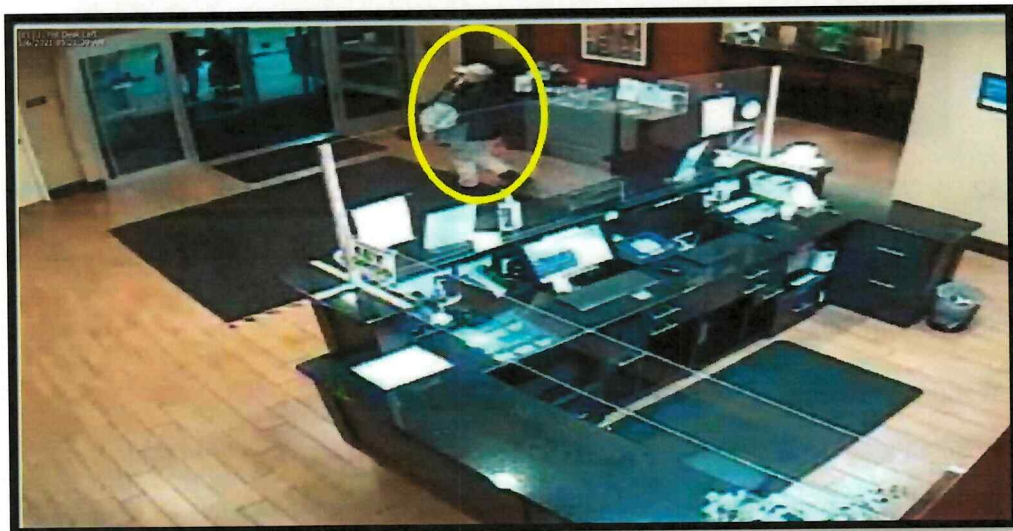
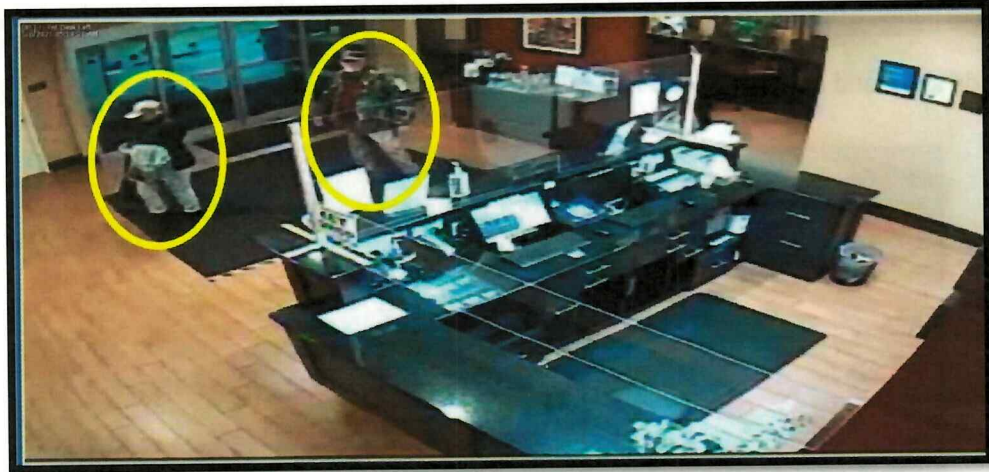
52. A search of Watkins's cellular phone revealed several messages between Watkins and "Recruit Ben – OSRM" (believed to be Bennie Parker) on the morning of January 6, 2021. In particular, the following text messages were identified:

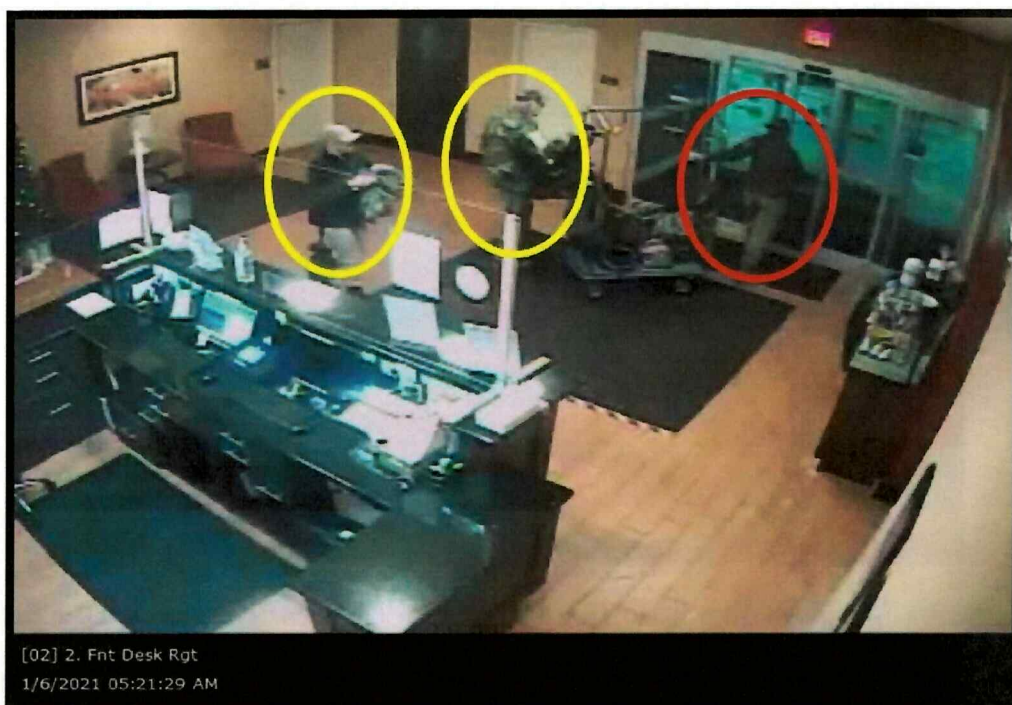
Watkins to Bennie Parker: Y'all up and getting ready?

Bennie Parker to Watkins: Yep

Watkins to Bennie Parker: Grabbing gear and heading to van

53. Surveillance footage from the Comfort Inn shows that on January 6, 2021, between 5:00 a.m. and 5:25 a.m., Sandra Parker and Bennie Parker (yellow circles) were in the Comfort Inn lobby and met with individuals who appear to be Watkins and Crowl (red circles). In the still frames, Sandra Parker is seen carrying a light-colored jacket with a possible camouflage pattern. Bennie Parker is observed wearing a camouflage patterned jacket.





54. During the search of Watkins's cellular phone, the FBI obtained several photographs, including images depicting an individual who appears to be Sandra Parker. In one of the photographs outside of the U.S. Capitol, the individual who appears to be Sandra Parker is seen wearing a tactical helmet and goggles, dark sunglasses, a light-colored camouflage jacket, and a black backpack. This image also depicts an individual who appears to be Bennie Parker, who is partially in the photo and seen wearing a tactical helmet and goggles. Both are standing next to an individual wearing a tactical vest with "Oath Keepers" emblazoned on it.



55. A January 29, 2021, New York Times article¹¹ entitled “Tracking the Oath Keepers Who Attacked the Capitol,” contained photos and videos depicting individuals who appear to be Sandra Parker and Bennie Parker. One such video shows an individual, who is believed to be Bennie Parker, marching toward the U.S. Capitol wearing a camouflage jacket, tan tactical vest, goggles with a subdued Ohio state flag patch, and a tactical helmet affixed with a “MILITIA” patch on the back.



¹¹ See <https://www.nytimes.com/interactive/2021/01/29/us/oath-keepers-capitol-riot.html> (last viewed on February 1, 2021)

56. In that same video, a woman walking in front of Bennie Parker is also wearing a tactical helmet with a “MILITIA” patch and goggles with a subdued Ohio state flag patch. The below pictures depict this individual wearing dark sunglasses, a light-colored camouflage jacket, and a black backpack. These photos resemble Sandra Parker’s known photo.



57. The below photo taken by a photojournalist who was present inside the Capitol on January 6, 2021, appears to show Sandra Parker (orange arrow)—wearing a tactical helmet and goggles, dark sunglasses, a camouflage jacket, and a black backpack—is standing behind Crowl

(red circle) and other Oath Keeper members, within the Rotunda:



58. Another photograph from the photojournalist appears to show Sandra Parker sitting inside the Capitol while wearing the same clothing and combat gear described above:



59. The search of Watkins's cellular phone revealed additional communications with Bennie Parker. In one exchange on January 6, 2021, at 5:43 p.m., Bennie Parker asked Watkins, "Is Sandi ok are tou ok?"

60. Following the events of January 6, 2021, Watkins and Bennie Parker texted each other about the ensuing federal investigation. Specifically, on January 9, 2021, and on January 14, 2021, they exchanged the following messages:

Watkins to Bennie Parker (1/9/21): I've been following FBI wanted list, seems they're only interested in people who destroyed things. I wouldn't worry about them coming after us

Bennie Parker to Watkins (1/9/21): I'm sure they're not on us see some pics but no militia

Bennie Parker to Watkins (1/9/21): Sandi was having sinus problems before we got to DC but she is starting to get a little better

Watkins to Bennie Parker (1/9/21): Good to hear. I didn't know that. She's a super trooper pushing through all that walking like she did!

Bennie Parker to Watkins (1/14/21): Hay I got to ask did you put Sandi out there in the Capital?

61. Beginning on or about February 8, 2021, law-enforcement officers conducted surveillance of the PREMISES. During surveillance, law-enforcement officers observed Sandra Parker's and Bennie Parker's known vehicles parked in the driveway of the PREMISES.

62. As explained in the preceding paragraphs, both Sandra and Bennie Parker were wearing distinctive clothing and protective/tactical gear on the date of the alleged offenses. Based on my training and experience, I know that individuals tend to store their clothing and other personal belongings in their homes. Additionally, the above paragraphs describe in greater detail a number of communications between Bennie Parker and others referring and relating to the Subject Offenses. Based on my training and experience, I know that individuals tend to communicate, and access and post to social-media sites, through digital devices, to include but not limited to, cellular telephones, tablets, and computers. Additionally, there is reason to believe that Sandra Parker and Bennie Parker, among other individuals affiliated with the Oath Keepers, likely

used the Zello app to communicate on January 6, 2021, during the commission of the Subject Offenses, and as mentioned above Zello is an app for digital devices that allows such devices to act as walkie-talkies. Finally, this investigation has revealed that Sandra Parker and Bennie Parker stayed at a hotel in Washington, D.C., during the period including January 6, 2021. I am aware that many individuals use digital devices to book travel accommodations, either through their computer or tablet or cellular telephone. I know that individuals tend to keep their digital devices on their person, or, when they are at home, nearby them at home.

TECHNICAL TERMS

63. Based on my training and experience, and information acquired from other law enforcement officials with technical expertise, I know the terms described below have the following meanings or characteristics:

a. “Digital device,” as used herein, includes the following three terms and their respective definitions:

1) A “computer” means an electronic, magnetic, optical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. *See* 18 U.S.C. § 1030(e)(1). Computers are physical units of equipment that perform information processing using a binary system to represent information. Computers include, but are not limited to, desktop and laptop computers, smartphones, tablets, smartwatches, and binary data processing units used in the operation of other products like automobiles.

2) “Digital storage media,” as used herein, means any information storage device in which information is preserved in binary form and includes electrical, optical, and magnetic digital storage devices. Examples of digital storage media include, but are not

limited to, compact disks, digital versatile disks (“DVDs”), USB flash drives, flash memory cards, and internal and external hard drives.

3) “Computer hardware” means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

b. “Wireless telephone” (or mobile telephone, or cellular telephone), a type of digital device, is a handheld wireless device used for voice and data communication at least in part through radio signals and also often through “wi-fi” networks. When communicating via radio signals, these telephones send signals through networks of transmitters/receivers, enabling communication with other wireless telephones, traditional “land line” telephones, computers, and other digital devices. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of applications and capabilities. These include, variously: storing names and phone numbers in electronic “address books”; sending, receiving, and storing text messages, e-mail, and other forms of messaging; taking, sending, receiving, and storing still photographs and video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; utilizing global

positioning system (“GPS”) locating and tracking technology, and accessing and downloading information from the Internet.

c. A “tablet” is a mobile computer, typically larger than a wireless phone yet smaller than a notebook, that is primarily operated by touch-screen. Like wireless phones, tablets function as wireless communication devices and can be used to access the Internet or other wired or wireless devices through cellular networks, “wi-fi” networks, or otherwise. Tablets typically contain programs called applications (“apps”), which, like programs on both wireless phones, as described above, and personal computers, perform many different functions and save data associated with those functions.

d. A “GPS” navigation device, including certain wireless phones and tablets, uses the Global Positioning System (generally abbreviated “GPS”) to display its current location, and often retains records of its historical locations. Some GPS navigation devices can give a user driving or walking directions to another location, and may contain records of the addresses or locations involved in such historical navigation. The GPS consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

e. “Computer passwords and data security devices” means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a

string of alpha-numeric characters) usually operates as a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

f. “Computer software” means digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g. Internet Protocol (“IP”) Address is a unique numeric address used by digital devices on the Internet. An IP address, for present purposes, looks like a series of four numbers, each in the range 0-255, separated by periods (*e.g.*, 149.101.1.32). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

h. The “Internet” is a global network of computers and other electronic devices that communicate with each other using numerous specified protocols. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

i. “Internet Service Providers,” or “ISPs,” are entities that provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers,

including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet, including via telephone-based dial-up and broadband access via digital subscriber line (“DSL”), cable, dedicated circuits, fiber-optic, or satellite. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name, a user name or screen name, an e-mail address, an e-mail mailbox, and a personal password selected by the subscriber. By using a modem, the subscriber can establish communication with an ISP and access the Internet by using his or her account name and password.

j. A “modem” translates signals for physical transmission to and from the ISP, which then sends and receives the information to and from other computers connected to the Internet.

k. A “router” often serves as a wireless Internet access point for a single or multiple devices, and directs traffic between computers connected to a network (whether by wire or wirelessly). A router connected to the Internet collects traffic bound for the Internet from its client machines and sends out requests on their behalf. The router also distributes to the relevant client inbound traffic arriving from the Internet. A router usually retains logs for any devices using that router for Internet connectivity. Routers, in turn, are typically connected to a modem.

l. “Domain Name” means the common, easy-to-remember names associated with an IP address. For example, a domain name of “www.usdoj.gov” refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first-level, or top-level domains are typically .com for commercial

organizations, .gov for the governmental organizations, .org for organizations, and .edu for educational organizations. Second-level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government.

m. “Cache” means the text, image, and graphic files sent to and temporarily stored by a user’s computer from a website accessed by the user in order to allow the user speedier access to and interaction with that website in the future.

n. “Peer to Peer file sharing” (P2P) is a method of communication available to Internet users through the use of special software, which may be downloaded from the Internet. In general, P2P software allows a user to share files on a computer with other computer users running compatible P2P software. A user may obtain files by opening the P2P software on the user’s computer and searching for files that are currently being shared on the network. A P2P file transfer is assisted by reference to the IP addresses of computers on the network: an IP address identifies the location of each P2P computer and makes it possible for data to be transferred between computers. One aspect of P2P file sharing is that multiple files may be downloaded at the same time. Another aspect of P2P file sharing is that, when downloading a file, portions of that file may come from multiple other users on the network to facilitate faster downloading.

i. When a user wishes to share a file, the user adds the file to shared library files (either by downloading a file from another user or by copying any file into the shared directory), and the file’s hash value is recorded by the P2P software.

The hash value is independent of the file name; that is, any change in the name of the file will not change the hash value.

ii. Third party software is available to identify the IP address of a P2P computer that is sending a file. Such software monitors and logs Internet and local network traffic.

o. “VPN” means a virtual private network. A VPN extends a private network across public networks like the Internet. It enables a host computer to send and receive data across shared or public networks as if they were an integral part of a private network with all the functionality, security, and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two. The VPN connection across the Internet is technically a wide area network (WAN) link between the sites. From a user perspective, the extended network resources are accessed in the same way as resources available from a private network-hence the name “virtual private network.” The communication between two VPN endpoints is encrypted and usually cannot be intercepted by law enforcement.

p. “Encryption” is the process of encoding messages or information in such a way that eavesdroppers or hackers cannot read it but authorized parties can. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, turning it into an unreadable ciphertext. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any unintended party that can see the ciphertext should not be able to determine anything about the original message. An authorized party, however, is able to decode the ciphertext using a decryption algorithm that usually requires a secret decryption key, to which adversaries do not have access.

q. “Malware,” short for malicious (or malevolent) software, is software used or programmed by attackers to disrupt computer operations, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. Malware is a general term used to refer to a variety of forms of hostile or intrusive software.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

64. As described above and in Attachment B, this application seeks permission to search for evidence, fruits, contraband, instrumentalities, and information that might be found on the PREMISES, in whatever form they are found. One form in which such items might be found is data stored on one or more digital devices. Such devices are defined above and include any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Thus, the warrant applied for would authorize the seizure of digital devices or, potentially, the copying of stored information, all under Rule 41(e)(2)(B). Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit that, if digital devices are found on the PREMISES, there is probable cause to believe that the items described in Attachment

B will be stored in the Device(s) for at least the following reasons:

a. Individuals who engage in criminal activity, including violations of the Subject Offenses, use digital devices, like the Device(s), in furtherance of these offenses, to plan, coordinate, and document these offenses, which can include logs of online chats with co-conspirators; email correspondence; text or other “Short Message Service” (“SMS”) messages; contact information of co-conspirators, including telephone numbers, email addresses, identifiers for instant messaging and social medial accounts; stolen financial and personal identification data, including bank account numbers, credit card numbers, and names, addresses, telephone numbers, and social security numbers of other individuals; and records of illegal transactions using stolen financial and personal identification data, to, among other things, (1) keep track of co-conspirator’s contact information; (2) keep a record of illegal transactions for future reference; (3) keep an accounting of illegal proceeds for purposes of, among other things, splitting those proceeds with co-conspirators; and (4) store stolen data for future exploitation. As described in greater detail above, law enforcement has uncovered evidence that Sandra Parker and Bennie Parker communicated with individuals affiliated with the Oath Keepers and used Zello, among other apps, to communicate about the roles of co-conspirators in the storming of the Capitol on January 6, 2021.

b. Individuals who engage in the foregoing criminal activity, in the event that they change digital devices, will often “back up” or transfer files from their old digital devices to that of their new digital devices, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity.

c. Digital device files, or remnants of such files, can be recovered months or even many years after they have been downloaded onto the medium or device, deleted, or viewed

via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person “deletes” a file on a digital device such as a home computer, a smart phone, or a memory card, the data contained in the file does not actually disappear; rather, that data remains on the storage medium and within the device unless and until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the digital device that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a digital device’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve “residue” of an electronic file from a digital device depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer, smart phone, or other digital device habits.

65. As further described in Attachment B, this application seeks permission to locate not only electronic evidence or information that might serve as direct evidence of the crimes described in this affidavit, but also for forensic electronic evidence or information that establishes how the digital device(s) were used, the purpose of their use, who used them (or did not), and when. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices,

I respectfully submit there is probable cause to believe that this forensic electronic evidence and information will be in any of the Device(s) at issue here because:

a. Although some of the records called for by this warrant might be found in the form of user-generated documents or records (such as word processing, picture, movie, or texting files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials contained on the digital device(s) are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive, flash drive, memory card, or other electronic storage media image as a whole. Digital data stored in the Device(s), not currently associated with any file, can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on a hard drive that show what tasks and processes on a digital device were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on a hard drive, flash drive, memory card, or memory chip that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times a computer, smart phone, or other digital device was in use. Computer, smart phone, and other digital device file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this

data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

b. Forensic evidence on a digital device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, chats, instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time, and potentially who did not.

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how such digital devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital device evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on digital devices is evidence may depend on other information stored on the devices and the application of knowledge about how the devices behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on the device. For example, the presence or absence of counter-forensic programs,

anti-virus programs (and associated data), and malware may be relevant to establishing the user's intent and the identity of the user.

METHODS TO BE USED TO SEARCH DIGITAL DEVICES

66. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I know that:

a. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time, in part because there are so many types of digital devices and software programs in use today. Digital devices – whether, for example, desktop computers, mobile devices, or portable storage devices – may be customized with a vast array of software applications, each generating a particular form of information or records and each often requiring unique forensic tools, techniques, and expertise. As a result, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched, and to obtain specialized hardware and software solutions to meet the needs of a particular forensic analysis.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover “hidden,” erased, compressed, encrypted, or password-protected data. Recovery of “residue” of electronic files from digital devices also requires specialized tools and often substantial time. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is often essential to conducting a complete and accurate analysis of data stored on digital devices.

c. Further, as discussed above, evidence of how a digital device has been used, the purposes for which it has been used, and who has used it, may be reflected in the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data or software on a digital device is not segregable from the digital device itself. Analysis of the digital device as a whole to demonstrate the absence of particular data or software requires specialized tools and a controlled laboratory environment, and can require substantial time.

d. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear as though the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or deliberately misspelling words, thereby thwarting “keyword” search techniques and necessitating continuous modification of keyword terms. Moreover, certain file formats, like portable document format (“PDF”), do not lend themselves to keyword searches. Some applications for computers, smart phones, and other digital devices, do not store data as searchable text; rather, the data is saved in a proprietary non-text format. Documents printed by a computer, even if the document was never saved to the hard drive,

are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography, a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband, or instrumentalities of a crime.

e. Analyzing the contents of mobile devices, including tablets, can be very labor intensive and also requires special technical skills, equipment, and software. The large, and ever increasing, number and variety of available mobile device applications generate unique forms of data, in different formats, and user information, all of which present formidable and sometimes novel forensic challenges to investigators that cannot be anticipated before examination of the device. Additionally, most smart phones and other mobile devices require passwords for access. For example, even older iPhone 4 models, running IOS 7, deployed a type of sophisticated encryption known as “AES-256 encryption” to secure and encrypt the operating system and application data, which could only be bypassed with a numeric passcode. Newer cell phones employ equally sophisticated encryption along with alpha-numeric passcodes, rendering most smart phones inaccessible without highly sophisticated forensic tools and techniques, or assistance from the phone manufacturer. Mobile devices used by individuals engaged in criminal activity are often further protected and encrypted by one or more third party applications, of which there are many. For example, one such mobile application, “Hide It Pro,” disguises itself as an audio

application, allows users to hide pictures and documents, and offers the same sophisticated AES-256 encryption for all data stored within the database in the mobile device.

f. Based on all of the foregoing, I respectfully submit that searching any digital device for the information, records, or evidence pursuant to this warrant may require a wide array of electronic data analysis techniques and may take weeks or months to complete. Any pre-defined search protocol would only inevitably result in over- or under-inclusive searches, and misdirected time and effort, as forensic examiners encounter technological and user-created challenges, content, and software applications that cannot be anticipated in advance of the forensic examination of the devices. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques reasonably appear to be necessary to locate and retrieve digital information, records, or evidence within the scope of this warrant.

67. The volume of data stored on many digital devices will typically be so large that it will be extremely impractical to search for data during the physical search of the premises.

a. Therefore, in searching for information, records, or evidence, further described in Attachment B, law enforcement personnel executing this search warrant will employ the following procedures:

1. Upon securing the PREMISES, law enforcement personnel will, consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, seize any digital devices (that is, the Device(s)), within the scope of this warrant as defined above, deemed capable of containing the information, records, or evidence described in Attachment B and transport these items to an appropriate law enforcement laboratory or similar facility for review. For all the reasons described above, it would not be feasible to conduct a complete, safe, and appropriate search of any such digital devices at the PREMISES. The digital devices, and/or any digital images

thereof created by law enforcement sometimes with the aid of a technical expert, in an appropriate setting, in aid of the examination and review, will be examined and reviewed in order to extract and seize the information, records, or evidence described in Attachment B.

2. The analysis of the contents of the digital devices may entail any or all of various forensic techniques as circumstances warrant. Such techniques may include, but shall not be limited to, surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); conducting a file-by-file review by “opening,” reviewing, or reading the images or first few “pages” of such files in order to determine their precise contents; “scanning” storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic “keyword” searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

3. In searching the digital devices, the forensic examiners may examine as much of the contents of the digital devices as deemed necessary to make a determination as to whether the contents fall within the items to be seized as set forth in Attachment B. In addition, the forensic examiners may search for and attempt to recover “deleted,” “hidden,” or encrypted data to determine whether the contents fall within the items to be seized as described in Attachment B. Any search techniques or protocols used in searching the contents of the seized digital devices will be specifically chosen to identify the specific items to be seized under this warrant.

BIOMETRIC ACCESS TO DEVICE(S)

68. This warrant permits law-enforcement agents to obtain from the persons of Sandra

Parker and Bennie Parker (but not any other individuals present at the PREMISES at the time of execution of the warrant) the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Device(s) requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned person(s)' physical biometric characteristics will unlock the Device(s). The grounds for this request are as follows:

69. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

70. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

71. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the

user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers (such as Apple's "Face ID") have different names but operate similarly to Trusted Face.

72. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

73. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

74. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices, the Device(s), will be found during the search. The passcode or password that would unlock the Device(s) subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data

contained within the Device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

75. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

76. Due to the foregoing, if law enforcement personnel encounter any Device(s) that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to obtain from the aforementioned person(s) the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Device(s), including to (1) press or swipe the fingers (including thumbs) of the aforementioned person(s) to the fingerprint scanner of the Device(s) found at the PREMISES; (2) hold the Device(s) found at the PREMISES in front of the face of the aforementioned person(s) to activate the facial recognition feature; and/or (3) hold the Device(s) found at the PREMISES in front of the face of the aforementioned person(s)

to activate the iris recognition feature, for the purpose of attempting to unlock the Device(s) in order to search the contents as authorized by this warrant.

77. The proposed warrant does not authorize law enforcement to require that the aforementioned person(s) state or otherwise provide the password, or identify specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the Device(s). Nor does the proposed warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person(s) to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person(s) would be permitted under the proposed warrant. To avoid confusion on that point, if agents in executing the warrant ask any of the aforementioned person(s) for the password to any Device(s), or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any Device(s), the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

CONCLUSION


I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

REQUEST FOR SEALING

It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation into the criminal organizations as not all of the

targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,


T. A. Staderman II
Special Agent
Federal Bureau of Investigation

Subscribed and sworn before me via telephone pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3) on February 17 2021.


Karen L. Litkovitz
United States Magistrate Judge



ATTACHMENT A

Property to be searched

The property to be searched is 1170 Essex Glenn, Morrow, Ohio, 45152 further described as a brick-and-siding two-story home, with a garage on the left side of the home, with a mailbox near the road with the numbers “1170” affixed to it. The photographs below depict the property to be searched.





ATTACHMENT B

Property to be seized

1. All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of 18 U.S.C. §§ 1512(c)(2) (obstruction of Congress); 1519 (obstruction of justice – destruction of evidence); 111 (assaulting a federal agent); 231 (civil disorders); 371 (conspiracy); 372 (conspiracy to impede/assault federal agents); 641 (theft of government property); 930 (possession of firearms and dangerous weapons in federal facilities); 1361 (destruction of government property); 1752(a) (unlawful entry on restricted buildings or grounds); 2101 (interstate travel to participate in riot); 2383 (rebellion or insurrection); and 2384 (seditious conspiracy); and 40 U.S.C. § 5104(e)(2) (violent entry, disorderly conduct, and other offenses on capitol grounds) that have been committed by Sandra Parker and Bennie Parker, and other identified and unidentified persons (collectively, the “SUBJECT OFFENSES”), as described in the affidavit submitted in support of this Warrant, occurring between November 3, 2020, and the present, including:

- a. Records and information that constitute evidence of use, control, ownership, or occupancy of the PREMISES and things therein;
- b. Evidence of the Subject Offenses, to include clothing, protective/tactical gear worn during the offenses, and firearms and other weapons;
- c. Evidence tending to show that Sandra Parker and Bennie Parker traveled to Washington, D.C., for a period to include on or about January 6, 2021, including travel reservations and receipts;

- d. Items used in furtherance of the Subject Offenses, to include digital devices, radios, and walkie-talkies, among other items;
- e. Records and information relating to a conspiracy to unlawfully enter the United States Capitol and to disrupt the certification of the 2020 Electoral College vote;
- f. Records and information that constitute evidence concerning persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation; or (ii) communicated with Sandra Parker and Bennie Parker about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts;
- g. Records and information that constitute evidence of the state of mind of Sandra Parker and Bennie Parker, *e.g.*, intent, absence of mistake, or evidence indicating preparation or planning, or knowledge and experience, related to the criminal activity under investigation; and
- h. Any evidence tending to show consciousness of guilt, including communications after January 6, 2021, about the Subject Offenses committed that day.

2. For any digital device which is capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities as described in the search warrant affidavit and above, hereinafter the "Device(s)":

- a. evidence of who used, owned, or controlled the Device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, chat, instant messaging logs, photographs, and correspondence;

- b. evidence of software, or the lack thereof, that would allow others to control the Device(s), such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the attachment to the Device(s) of other storage devices or similar containers for electronic evidence;
- d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Device(s);
- e. evidence of the times the Device(s) was used;
- f. passwords, encryption keys, and other access devices that may be necessary to access the Device(s);
- g. documentation and manuals that may be necessary to access the Device(s) or to conduct a forensic examination of the Device(s);
- h. records of or information about Internet Protocol addresses used by the Device(s);
- i. records of or information about the Device(s)'s Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

3. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

4. The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

5. The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

6. The United States government will conduct a search of the property described in Attachment A and determine which information is within the scope of the information to be seized specified above. That information that is within the scope of this warrant may be copied and retained by the United States.

7. Law enforcement personnel will then seal any information from the property searched that does not fall within the scope of this warrant and will not further review the information absent an order of the Court. Such sealed information may include retaining a digital copy of all information received pursuant to the warrant to be used for authentication at trial, as needed.

8. This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff

for their independent review.

9. During the execution of the search of the PREMISES described in Attachment A, law enforcement personnel are also specifically authorized to obtain from Sandra Parker and Bennie Parker (but not any other individuals present at the PREMISES at the time of execution of the warrant) the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint, facial characteristics, or iris display) necessary to unlock any Device(s) requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned person(s)' physical biometric characteristics will unlock the Device(s), to include pressing fingers or thumbs against and/or putting a face before the sensor, or any other security feature requiring biometric recognition of:

- (a) any of the Device(s) found at the PREMISES,
- (b) where the Device(s) are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments,

for the purpose of attempting to unlock the Device(s)'s security features in order to search the contents as authorized by this warrant.

10. While attempting to unlock the device by use of the compelled display of biometric characteristics pursuant to this warrant, law enforcement is not authorized to demand that the aforementioned person(s) state or otherwise provide the password or identify the specific biometric characteristics (including the unique finger(s) or other physical features), that may be used to unlock or access the Device(s). Nor does the warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to

compel the aforementioned person(s) to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person(s) is permitted. To avoid confusion on that point, if agents in executing the warrant ask any of the aforementioned person(s) for the password to any Device(s), or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any Device(s), the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.